

APPLICATION SANDBOXING

PRINCIPLES, TECHNOLOGIES, AND SECURE ISOLATION



NAMESPACES
& CGROUPS



CONTAINERS



VIRTUAL
MACHINES



MICROVMS



WEBASSEMBLY



BROWSER
SANDBOXES



CONFIDENTIAL
COMPUTING



ISOLATED
EXECUTION



MINIMAL
ATTACK
SURFACE



PRIVILEGE
BOUNDARIES



AUDITABLE
& CONTAINED

STEVE T.

Application Sandboxing

Principles, Technologies, and Secure Isolation

Steve T. Team Publications

This book is available at <https://leanpub.com/applicationsandboxing>

This version was published on 2026-07-03



This is a [Leanpub](#) book. Leanpub empowers authors and publishers with the Lean Publishing process. [Lean Publishing](#) is the act of publishing an in-progress ebook using lightweight tools and many iterations to get reader feedback, pivot until you have the right book and build traction once you do.

© 2026 Steve T. Team Publications

Contents

Principles, Technologies, and Secure Isolation	1
Introduction: When Isolation Fails	2
The Promise of Sandboxing	2
What This Book Covers	2
What This Book Does Not Cover	2
How to Read This Book	2
A Note on the Evolving Landscape	2
Chapter 1: Why Sandboxing? – The Threat Model and the Promise of Isolation	3
The Cost of Unbounded Execution: Real Incidents	3
Blast Radius and the Defense-in-Depth Philosophy	3
A Taxonomy of Isolation Mechanisms	3
What This Book Will (and Won't) Cover	3
Chapter 2: The Kernel as Enforcer – Namespaces, Cgroups, and the Linux Sandboxing Stack	4
Namespaces: Partitioning What You See	4
Cgroups: Controlling What You Can Do	4
User Namespaces and Unprivileged Containers	4
Composing Isolation: From Primitives to Containers	4
Limitations and Known Gaps in Linux Isolation	4
Chapter 3: Mandatory Access Control – SELinux, AppArmor, and Smack	5
Discretionary vs Mandatory Access Control	5
SELinux: Architecture and Policy Model	5
AppArmor: Profile-Based Protection	5
Smack and Alternative MAC Frameworks	5
Operational Challenges and Adoption Barriers	5

Chapter 4: System Call Filtering – seccomp, Landlock, and Capability Dropping	6
Linux Capabilities: Fine-Grained Privilege Splitting	6
seccomp-bpf: Filtering the System Call Surface	6
Landlock: A New Era of Unprivileged Sandboxing	6
Composing Filters with Capability Dropping	6
Real-World seccomp Profiles and Case Studies	6
Chapter 5: eBPF – The Universal Sandbox Primitive	7
From TCPdump to Trusted Kernel Runtime: The eBPF Revolution	7
How eBPF Works: Verifier, Programs, and Maps	7
eBPF for Network and Filesystem Sandboxing	7
Observability-Driven Security with eBPF	7
Trust Boundaries and the eBPF Threat Model	7
The eBPF Security Model in Practice	7
Chapter 6: Container Runtimes and the OCI Ecosystem	9
The OCI Standard: Making Containers Portable	9
Docker Architecture Deep Dive	9
containerd and CRI-O: Kubernetes-Native Runtimes	9
Rootless Containers and User Namespace Remapping	9
Storage Drivers and Image Layers	9
Chapter 7: Virtual Machines and MicroVMs – Hardware-Level Isolation	10
Virtualization Fundamentals and the Hypervisor Stack	10
KVM and QEMU: The Linux Virtualization Foundation	10
MicroVMs: Firecracker, Crosvm, and the Edge of Performance	10
Security Comparison: VMs vs Containers	10
When to Choose Hardware Isolation Over OS-Level Sandboxing	10
Chapter 8: Desktop and Mobile Sandboxes – macOS, Windows, Android, iOS, and Browsers	11
macOS Sandbox: Seatbelt and Entitlements	11
Windows AppContainer and Virtual-Based Sandboxing	11
Android’s Per-App Isolation Model	11
iOS Application Sandboxing and Entitlements	11
Browser Sandboxes: Process Isolation and Site Separation	11
Chapter 9: Language and Runtime Sandboxes – From chroot to WebAssembly	13

chroot: The Oldest Trick in the Book	13
FreeBSD Jails: BSD's Isolation Philosophy	13
LXC and LXD: System Containers on Linux	13
WebAssembly and WASI: Sandboxing at the Bytecode Level	13
Language and Runtime Sandboxing Approaches	13
Chapter 10: Sandbox Escapes – How Isolation Fails and What to Do	
About It	15
Container Escape Techniques and Case Studies	15
VM Escape: Hypervisor Vulnerabilities and Side Channels	15
Browser Sandbox Bypasses	15
Desktop OS Sandbox Escapes	15
Defense Strategies and the Ongoing Arms Race	15
Chapter 11: Designing and Operating Sandboxed Environments	16
Threat Modeling Your Sandboxing Strategy	16
Selecting Isolation Technology for Different Workloads	16
Hardening Container Images and Runtimes	16
Network Segmentation and Zero-Trust Networking	16
Observability, Debugging, and Operational Excellence	16
Chapter 12: The Future of Sandboxing – Serverless, Confidential Computing, and Beyond	17
Serverless Isolation: The Function-as-a-Service Model	17
Confidential Computing: When the Kernel Can't Be Trusted	17
WebAssembly's Expanding Sandbox Horizon	17
The Convergence Playbook: Containers, VMs, and Wasm Together	17
Open Challenges and Where the Field Is Heading	17
Conclusion: The Principle of Measured Trust	19
References	20

Principles, Technologies, and Secure Isolation

About this book: This book is a comprehensive technical guide to application sandboxing in modern computing. It covers the theory, architecture, implementation, and security models behind every major isolation technology, from Linux namespaces and cgroups through containers, virtual machines, microVMs, WebAssembly, browser sandboxes, and confidential computing. You will learn how each approach works under the hood, what trade-offs it makes in security versus performance versus portability, how attackers bypass these boundaries, and how to select, implement, and harden sandboxing solutions for desktop, server, cloud-native, and embedded environments. Whether you are a systems engineer designing the next generation of secure infrastructure, a security professional hunting for escape vectors, or an application developer who needs to ship code that runs safely in shared environments, this book will give you the technical depth and practical guidance to make informed decisions about isolation.

Introduction: When Isolation Fails

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

The Promise of Sandboxing

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

What This Book Covers

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

What This Book Does Not Cover

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

How to Read This Book

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

A Note on the Evolving Landscape

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

Chapter 1: Why Sandboxing? – The Threat Model and the Promise of Isolation

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

The Cost of Unbounded Execution: Real Incidents

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

Blast Radius and the Defense-in-Depth Philosophy

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

A Taxonomy of Isolation Mechanisms

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

What This Book Will (and Won't) Cover

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

Chapter 2: The Kernel as Enforcer — Namespaces, Cgroups, and the Linux Sandboxing Stack

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

Namespaces: Partitioning What You See

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

Cgroups: Controlling What You Can Do

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

User Namespaces and Unprivileged Containers

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

Composing Isolation: From Primitives to Containers

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

Limitations and Known Gaps in Linux Isolation

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

Chapter 3: Mandatory Access Control

– SELinux, AppArmor, and Smack

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

Discretionary vs Mandatory Access Control

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

SELinux: Architecture and Policy Model

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

AppArmor: Profile-Based Protection

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

Smack and Alternative MAC Frameworks

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

Operational Challenges and Adoption Barriers

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

Chapter 4: System Call Filtering — seccomp, Landlock, and Capability Dropping

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

Linux Capabilities: Fine-Grained Privilege Splitting

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

seccomp-bpf: Filtering the System Call Surface

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

Landlock: A New Era of Unprivileged Sandboxing

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

Composing Filters with Capability Dropping

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

Real-World seccomp Profiles and Case Studies

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

Chapter 5: eBPF – The Universal Sandbox Primitive

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

From TCPdump to Trusted Kernel Runtime: The eBPF Revolution

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

How eBPF Works: Verifier, Programs, and Maps

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

eBPF for Network and Filesystem Sandboxing

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

Observability-Driven Security with eBPF

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

Trust Boundaries and the eBPF Threat Model

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

The eBPF Security Model in Practice

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

Chapter 6: Container Runtimes and the OCI Ecosystem

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

The OCI Standard: Making Containers Portable

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

Docker Architecture Deep Dive

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

containerd and CRI-O: Kubernetes-Native Runtimes

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

Rootless Containers and User Namespace Remapping

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

Storage Drivers and Image Layers

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

Chapter 7: Virtual Machines and MicroVMs – Hardware-Level Isolation

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

Virtualization Fundamentals and the Hypervisor Stack

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

KVM and QEMU: The Linux Virtualization Foundation

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

MicroVMs: Firecracker, Crosvm, and the Edge of Performance

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

Security Comparison: VMs vs Containers

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

When to Choose Hardware Isolation Over OS-Level Sandboxing

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

Chapter 8: Desktop and Mobile Sandboxes – macOS, Windows, Android, iOS, and Browsers

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

macOS Sandbox: Seatbelt and Entitlements

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

Windows AppContainer and Virtual-Based Sandboxing

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

Android's Per-App Isolation Model

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

iOS Application Sandboxing and Entitlements

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

Browser Sandboxes: Process Isolation and Site Separation

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

Chapter 9: Language and Runtime Sandboxes – From chroot to WebAssembly

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

chroot: The Oldest Trick in the Book

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

FreeBSD Jails: BSD's Isolation Philosophy

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

LXC and LXD: System Containers on Linux

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

WebAssembly and WASI: Sandboxing at the Bytecode Level

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

Language and Runtime Sandboxing Approaches

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

Chapter 10: Sandbox Escapes – How Isolation Fails and What to Do About It

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

Container Escape Techniques and Case Studies

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

VM Escape: Hypervisor Vulnerabilities and Side Channels

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

Browser Sandbox Bypasses

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

Desktop OS Sandbox Escapes

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

Defense Strategies and the Ongoing Arms Race

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

Chapter 11: Designing and Operating Sandboxed Environments

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

Threat Modeling Your Sandboxing Strategy

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

Selecting Isolation Technology for Different Workloads

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

Hardening Container Images and Runtimes

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

Network Segmentation and Zero-Trust Networking

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

Observability, Debugging, and Operational Excellence

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

Chapter 12: The Future of Sandboxing – Serverless, Confidential Computing, and Beyond

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

Serverless Isolation: The Function-as-a-Service Model

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

Confidential Computing: When the Kernel Can't Be Trusted

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

WebAssembly's Expanding Sandbox Horizon

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

The Convergence Playbook: Containers, VMs, and Wasm Together

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

Open Challenges and Where the Field Is Heading

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

Conclusion: The Principle of Measured Trust

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.

References

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/applicationsandboxing>.